Statement of Jawad Khaki

**Corporate Vice President,
Windows Networking and Device Technologies
Microsoft Corporation**

**Testimony Before the
Committee on Government Reform
U.S. House of Representatives**

June 29, 2005

**Hearing on "To Lead or Follow:
The Next Generation Internet and the Transition to IPv6"**

COMMENTS OF MICROSOFT CORPORATION

Introduction

Chairman Davis, Ranking Member Waxman and Members of the Committee: My name is Jawad Khaki, and I am the Corporate Vice President for Windows Networking and Device Technologies at Microsoft, responsible for the core Windows network team. I consider it a great honor to be with the Committee today, and look forward to working with the Committee to help ensure that America remains at the forefront of innovation and opportunity. Over the last decade Microsoft has worked closely with the government and our partners to help promote the growth of new, innovative Internet technologies and strengthen our domestic IT industry.

I have been at Microsoft for over 16 years, and have focused on network, software, and hardware design for the last 25 years. Beginning in July, I will also serve on the Federal Communications Commissions' Technical Advisory Council, which is designed to provide the FCC with technical advice on emerging technologies. In both this hearing today and as part of that Forum, my goal is to help America maintain its tradition of technological excellence and role as the global leader in information technology.

The current Internet Protocol, version 4 ("IPv4"), has fostered amazing growth of the Internet. Yet with the rapid growth of broadband technologies, the advent of new Internet-connected devices, and increasing concerns about the functionality and flexibility of the IPv4-based Internet, more advanced networking technologies are desirable.

A gradual, market-based conversion to IPv6 is the most technologically feasible and least disruptive way of addressing these concerns and realizing the full promise of the Internet. A strong partnership between government and industry is also critically important, as is a proactive national policy to promote IPv6.

This testimony first provides a brief historical overview of IPv4 and the significant role the government played in its creation and subsequent growth. It then highlights the successes other countries have had in promoting IPv6 development through government incentives and industry cooperation. Next, the testimony highlights why IPv6 is so important to the continued growth of our IT industry and how Microsoft is working hard to promote IPv6. The testimony concludes with a call to action for both industry and government.

A Brief Historical Perspective on IPv4 Deployment

The US government was instrumental in fostering the development and deployment of IPv4 which in turn helped propel the Internet to its current position as the main artery of communication and information sharing. Beginning in the late 1960's, the Advanced Research Projects Agency provided the funding to design and deploy the ARPANET, the predecessor to the Internet, and helped foster the development of IPv4. The National Science Foundation's support for NSFNet, a cross-country Internet backbone designed to help support government agencies, research, and educational activities, in the 1980's prompted rapid industry innovation in IPv4 networking technologies and devices.

By the early 1990's, independent commercial networks began to develop, using many of the same devices and applications produced for the NSFNet. When NSFNet sponsorship ended in the mid-1990's, the Internet's backbone and periphery networks moved into the private sector. Shortly thereafter, consumers and businesses moved quickly to the Internet, propelled by new technologies such as Microsoft's Windows 95, which supported the IPv4 protocol.

In summary, the success of the Internet today is due, in large part, to the efforts of the US government providing initial financial incentives, and Microsoft and other key industry partners providing Internet-capable devices and applications. Throughout this period, the United States maintained a strong leadership role in the technical development of the Internet's architecture, in developing IPv4 devices and applications, and in supporting private industry growth. We firmly believe that the United States must continue this tradition of proactive leadership as we move forward in our transition from IPv4 to IPv6.

Why IPv6 is Important

The United States has benefited greatly from an IPv4-driven Internet; it has propelled our academic research, made government more efficient and responsive, and enabled both US and international companies to grow the world economy. While other countries have also benefited from the growth of the Internet, it is only recently that countries besides the United States have begun focusing on next-generation networking technologies, most notably IPv6.

The reasons for this focus on IPv6 are understandable. Over 450 million people now have access to the Internet, and close to 300 million users actively use the Internet from a personal computer at home. Broadband Internet access is now commonly available worldwide, and the latest IP-based devices and services such as mobile telephones, multiplayer games, Voice over Internet Protocol (VoIP), videoconferencing and IP-based TVs are placing increasing demands on the Internet's performance. Indeed, many of the most innovative uses of the Internet now require a combination of high-speed network connectivity, sophisticated software, and advanced networking devices. This combination is most effectively realized through an IPv6-capable Internet. Appendix A describes some of the design limitations of the IPv4 protocol and highlights how IPv6 not only mitigates these limitations, but also provides other technical advantages, such as many orders of magnitude increase in the number of addresses available for network-connected users and devices.

International IPv6 Efforts

The most noteworthy and sophisticated IPv6 efforts outside of the United States are in Asia. Several factors have played a large role in the Asian push to move to a next-generation Internet architecture: 1) Asia has a smaller allocation of IPv4 address space than either North America or Europe, 2) Several Asian countries have deployed high-speed broadband Internet infrastructure which reaches a high percentage of their population, and 3) Advanced mobile devices and applications requiring Internet access are hugely popular among many Asian populations.

Japan is a particularly good example of active government involvement in IPv6 deployment. In September 2000, Prime Minister Mori Yoshiro made IPv6 a national priority, and by early 2001 Japan had initiated an "e-Japan" strategy that specifically called out the need for government support of IPv6 networks. Since that time, Japan has used cooperation with other Asian nations, economic incentives, policies supporting network security and consumer privacy, deregulation, and the digitization of government to help promote its IPv6 efforts to great effect. This strong push has prompted Japan's commercial sector to respond with rapid advances in network technologies and devices. We anticipate that Japan will roll out robust, commercial IPv6 networks capable of supporting tens of millions of broadband subscribers over the next few years. This Japanese effort is in many ways akin to the US government and industry partnership seen most prominently during the early development of the Internet.

In other parts of Asia, national governments are highly focused on growing their domestic IPv6 industries. For example, India's IT Ministry listed IPv6 as one of its ten IT next-generation communication and computing framework initiatives. The Chinese government created the China Next Generation Internet (CNGI) project fund to support the development of IPv6 Internet networks and support telecom operators developing IPv6 technologies. China's CERNET2 IPv6 project is designed to not only deploy IPv6 Internet technologies, but also to promote domestic industry; key suppliers of technology for this project are Chinese companies.

In addition to the ongoing Asian efforts, the European Community has supported IPv6 for several years through research and experimental network trials both regionally and with Asian countries, such as South Korea. We are increasingly seeing activity and interest from Europe's public and privacy sector, particularly with respect to military organizations.

<u>Marketplace Forces in the US Are Working to Deploy IPv6 at an Appropriate Pace</u>

IPv6 adoption has proceeded slowly in the United States, but is likely to accelerate as IPv6 network solutions and applications become more available, robust, and affordable. Due to the flexible nature of IPv6 from a deployment perspective, we see early IPv6 conversion activity taking place at the edge of the network such as in home computers, and gradually moving to encompass to rest of the global Internet infrastructure. Over the past 6 months, we have seen several US carriers and service providers making solid plans toward piloting and deploying IPv6 services.

While deploying IPv6 technologies offers significant promise, the conversion from IPv4 to IPv6 is a large task that ultimately will affect nearly all current IP-based network architectures, applications, systems, and operational procedures. Given the magnitude of the project and the lack of specific deadlines, hardware and software designers, network providers, and users are generally approaching the conversion from IPv4 to IPv6 judiciously to avoid costly missteps. From our perspective, it appears that private industry efforts are working well at this early stage of IPv6 planning and deployment; companies continue to support IPv4, increasingly provide IPv6 compatibility, and many are preparing for an eventual transition to an IPv6 network.

Cost For Migrating From IPv4 to IPv6

There will be significant costs associated with migrating from IPv4 to IPv6, but we anticipate that the net benefits of the migration will outweigh these costs. These benefits are detailed in Appendix A.

However, it is difficult to quantify an exact cost amount of either an individual or national-level IPv6 transition, since the costs will depend heavily on the way entities deploy IPv6. For example, support for IPv6 transitional technologies are provided as an inherent part of the protocol, and we believe these transitional technologies are the most cost-effective, fastest, and least disruptive way to introduce IPv6 connectivity into an existing IPv4 environment. Commercial products are available today to deploy these transitional technologies.

As a second example, a full native IPv6 deployment—one that does not use transitional technologies or a hybrid IPv4-IPv6 architecture—can be achieved through gradually adding IPv6 into the network through an entity's regular technology refresh cycle. This gradual process minimizes the cost associated with rapid hardware and software upgrades. Regardless of method of deployment, there will be "soft" costs such as employee training, documentation, and other non-technology costs as part of a transition to an IPv6 architecture.

Some of Microsoft's partners have already begun building IPv6-capable networks or have made progress toward understanding what is needed to support the new protocol. This includes both international partners, as well as US agencies such as the Department of Defense.

<u>Microsoft's Efforts to Promote IPv6-Enabled Software</u>

We are most familiar with our own efforts to promote IPv6 and help the global Internet community move from an IPv4-based Internet to an IPv6 environment. Microsoft is not a newcomer to IPv6; we have long understood its importance and have made a strong commitment to promote its adoption. Moving forward, we are committed to supporting our customers' needs and rollout schedules for IPv6 and ensuring that our product lines support IPv6. We remain acutely aware, however, that any IPv6 deployment should be a phased transition that results in minimal infrastructure upheaval for our partners and customers.

Microsoft's research and development efforts have participated and contributed to the Internet Engineering Task Force's IPv6 standard-setting activities since 1996, when the specifications for IPv6 were still in draft form. In early 1998, Microsoft made an early version of an IPv6 protocol available to the IPv6 standards development community in the hopes of building industry consensus.

We have been incorporating IPv6 technology into our existing software for the last five years:

- In March 2000, we released a technology preview for the Windows 2000 operating system. This preview allowed software developers to familiarize themselves with the capabilities of IPv6 and to enable applications to use IPv6.

- In October 2001, we released the Windows XP operating system with a developer preview of the IPv6 protocol. We enabled key components for IPv6 so that software developers could begin enabling applications to work with IPv6 only or both IPv4 and IPv6 together.
- In March 2003, we released Windows Server 2003 with the first edition of Microsoft's IPv6 production stack and IPv6-enabled components.
- In July 2003, we released the Advanced Networking Pack for Windows XP. This release contained IP-based tunneling technology that provided the ability to provide IPv6 addresses over IPv4-based NATs.
- In August 2004, Windows XP Service Pack 2 (SP2) was released. This service pack upgraded the XP IPv6 support to be full production quality, and also included integrated IPv6 traffic support with the new Windows Firewall.
- We are currently working on delivering the next-generation Windows operating system, code-named Longhorn. Longhorn will be fully IPv6-capable. We are also working toward developing a full set of IPv6-capable applications and services during the next major product release cycle.
- In our effort to deliver Longhorn and the Longhorn-wave of IPv6-capable products, Microsoft's IT organization has taken an aggressive approach toward piloting, deploying and testing IPv6 on our corporate network. This deployment includes deploying IPv6-aware applications and hardware and IPv6 transitional technologies. These internal deployments help us gain operational experience in deploying and simultaneously running IPv4 and IPv6 technologies on our corporate network. It also allows us to extensively test our products and services prior to release to the public.

Microsoft's Commitment to IPv6 Security

Our IPv6 strategy includes a strong commitment to security. For example, we believe that every computer must be able to protect itself against attacks, even if the computer is behind a firewall in an internal network. Our belief is based on the fact that many attacks today come from inside the organization or home, whether it's from a laptop or digital media device unknowingly carrying a virus, or due to a malicious internal user. Just like we all lock the front doors to our homes even though our national borders are protected, each computer must likewise protect itself from attacks within the network. For this reason, Windows XP SP2 includes a firewall for both IPv4 and IPv6 in every computer.

As a second example, the Microsoft IPv6 implementation includes IP layer security known as Internet Protocol Security (IPSec). IPSec is an industry standard security technology that provides for data authenticity and integrity as well as data confidentiality across the array of protocols used by devices and applications.

Thirdly, we are working with our industry partners to help ensure that IPv6 security is incorporated into current and next-generation security products and services such as intrusion detection systems and firewalls.

Lastly, our existing security technologies will continue to operate in hybrid environments where both IPv4 and IPv6 are used. In order for a network environment to be fully IPv6 enabled, both the operating system and application or service must be IPv6-enabled. But in a hybrid IPv4-IPv6 environment, this will not be the case. For example, in Windows XP and Windows Server 2003, even when IPv6 is enabled on the network many applications and services will only respond via IPv4. Under this situation, existing IPv4-based security mechanisms continue to protect the network traffic over IPv4.

<u>The US Government's Role with Respect to IPv6 Deployment</u>

Microsoft believes that software and hardware manufacturers will increasingly provide affordable IPv6 offerings that are attractive to the public and private sectors because of IPv6's technical merits. Thus, the ordinary operation of the commercial marketplace, which includes the government being an engaged customer, should gradually lead to widespread use of IPv6 in the United States and around the world.

In keeping with this government's role in the development and incubation of the ARPANET, NSFNet, and IPv4, we support an active and engaged government policy geared towards promoting IPv6 as the next generation networking protocol. We would not suggest mandates or regulations that favor one implementation of IPv6 over another, but we welcome efforts to strengthen our information technology economy and stimulate commercial innovation.

On the academic front, as Bill Gates stated at the Library of Congress in May, we support government funded basic research programs, including those that consider what the Internet will look like in the future. Our universities and laboratories must be invigorated with first-class research programs and thinkers to continue to blaze the technology trail. One practical way of doing this is promoting the inclusion of IPv6 in undergraduate and graduate coursework.

As noted earlier, several Asian governments and the EU are working with their commercial partners to stimulate faster adoption of IPv6. We suggest that these efforts be evaluated for consideration, particularly tax incentives and government-matched funding.

Another role that the US government can play is as a major purchaser of information technology software and hardware. US government procurement standards and requirements have a profound impact on commercial product strategy and delivery plans. State and local governments, and even commercial entities, often base their IT purchases on the federal government. Thus strong IPv6 support from the US government, such as current efforts by the Department of Defense, will only strengthen the perception that IPv6 is a trusted, legitimate technology that should be in the future plans of American business and the public sector.

Conclusion

I sincerely hope the Committee has found these comments helpful as it evaluates the US transition from IPv4 to IPv6. Assuming continued exponential growth in both the number of devices connected to the Internet and the overall level of network traffic, IPv6 conversion is a necessary step to sustain the health and realize the full promise of the Internet. Microsoft is excited about IPv6's potential to enhance the computing and communication experiences of users around the world and hope that the US government will continue its long tradition of promoting innovation in the IT industry by supporting the development and implementation of IPv6 technologies. We look forward to working with this Committee and our partners to ensure that the US continues to be drive innovation and growth in IPv6 specifically and in our industry generally. If you need further information, I would be happy to speak before the committee at a later date or work with your staff to answer more specific questions about IPv6.

Appendix A: Overview of IPv4 and IPv6

<u>Overview of Internet Protocol Version 4 (IPv4) and Its Weaknesses</u>

The Internet Protocol ("IP") is the international standard protocol that defines how data is sent from one computer or device to another over the Internet. While that function sounds simple, the technical details of using and deploying IP are quite complex. In addition, because IP is fundamental to Internet connectivity, and is implemented in so many kinds of software and hardware, a change in IP is no simple task.

IPv4 was developed over 30 years ago, and has now been in use for over 20 years. During that time, the Internet has grown from a small network for a relatively few researchers and government contractors to an indispensable and nearly ubiquitous avenue of communication, commerce and entertainment for governments, educational institutions, corporations, and individuals.

This boom in Internet usage and the accompanying new demands on Internet service have underscored design weaknesses in IPv4 that are already beginning to affect the quality of service Internet users enjoy. These weaknesses include:

- <u>*A lack of adequate address space to meet fast-growing demand*</u>. IPv4 provides recognition of up to four billion addresses. While that number seems virtually unlimited, IP addresses have been rationed using short-term organization-specific solutions since the early 1990's. These solutions have been quite successful and have removed the appearance of IP scarcity for the average user. However, these solutions were not intended to be permanent, and the supply of addresses will face increasing pressure over time.

- *Address-conservation techniques that limit end-to-end connectivity between computers and other devices*. To make the most out of limited address space, some users have adopted workaround technologies such as Network Address Translators ("NATs"), which map a single IP address to several private addresses. However, these technologies interfere with many of today's applications, making the Internet difficult to use for many users, and also interfere with efforts to provide end-to-end security.
- *Growing numbers of addresses that burden the means of routing communications*. The Internet's routing tables and other means of routing network communications are becoming increasingly burdened and inefficient due to the sheer number of Internet addresses and the related practices for allocating these addresses. The resulting costs and delays may prove to be a larger problem than IPv4's constraints on the absolute number of available addresses.
- *The need to support new network services that did not exist when IPv4 was developed.* Technology advances and the evolution of the Internet over the last 20 years have led to new requirements in areas such as security, mobility and quality of service that IPv4's design did not take into account. While it is possible to substantially address these requirements in IPv4, such work-around solutions can be complex, costly, and inefficient.
- *A lack of integrated security.* Since IPSec was created after IPv4's standardization, many current IPv4 devices do not support IP-layer security. In addition, some elements of the IPv4 protocol such as ARP cannot be evolved to meet the security challenges posed by modern-day technologies such as wireless LANs.

<u>Internet Protocol Version 6 (IPv6) and Its Advantages</u>

IPv6 was designed to overcome the weaknesses of IPv4 described above, to enable new computing and communications paradigms, and to provide a flexible and operationally robust platform for future Internet growth. IPv6's advantages over IPv4 include:

- *<u>IPv6 positions the Internet for future growth</u>*. IPv6 increases the size of each address from 32 to 128 bits, vastly increasing the number of available addresses and virtually eliminating the need for NATs and other address-conservation techniques with their attendant disadvantages.
- *<u>IPv6 supports end-to-end connectivity</u>*. Because every individual device connected to the Internet will be able to have its own IP address, IPv6 promotes speed and quality of service and facilitates applications such as IP telephony and video teleconferencing. IPv6 also restores the original objective of Internet architecture to enable end-to-end communications by permitting routing of communications around failures in the network.
- *<u>IPv6 provides a framework for end-to-end trustworthy networking</u>*. Through built-in security and support for authentication and privacy capabilities, IPv6 promotes end-to-end trustworthy networking, and thus provides better resistance to attacks.
- *<u>IPv6 will enable more efficient routing of network communications</u>*. IPv6's large address space can be allocated in a hierarchical manner that reflects the current topology of the Internet. This hierarchical allocation and its better route aggregation framework should permit greater efficiency in the routing of network communications.

- *IPv6 better handles mobile applications and services*. IPv6 provides native redirection features and capabilities for facilitating device and user movement. These features better enable mobility of networked wireless services and simplify the design and construction of wireless networks. This same technology can also help the industry to develop application and services through innovative use of IP addresses.
- *IPv6 permits easier networking*. IPv6 offers a stateless autoconfiguration feature that will allow “plug and play” use of devices.
- *IPv6 enables exciting new products and services*. These features will allow developers to offer exciting IP-based applications that fundamentally change users’ Internet experience.